Please amend the present application as follows:

In the Specification

The following is a marked-up version of the specification with the language that is underlined ("___") being added and the language that contains strikethrough ("—") being deleted:

For the paragraph beginning on page 1, line 21, please substitute the following amended paragraph:

"The Rijndael algorithm, which was developed by Joan Daemen and Vincent Rijmen, is described in detail in their proposal "The Rijndael Block Cipher - AES Proposal: Rijndael" (hereinafter referred to as the "Rijndael proposal" or the "AES proposal") to the National Institute of Standards and Technology (NIST). While not all of the details are provided herein, the following provides the relevant portions of the AES algorithm."

For the paragraphs beginning at page 8, line 13, please amend as follows:

"FIG. 7A is a block diagram showing an example hardware configuration of the system of the invention having an optimized cipher subprocessor.

FIG. 7B is a block diagram showing an example hardware configuration of the system of the invention having an optimized cipher subprocessor.

FIG. 7C is a block diagram showing an example hardware configuration of the system of the invention having an optimized cipher subprocessor."

For the paragraph beginning on page 8, line 23, please substitute the following amended paragraph:

"FIG. 11A is a diagram showing another embodiment of the system of the invention having a hardwired S-box within the cipher subprocessor of FIG. 7B."

For the paragraph beginning on page 9, line 4, please substitute the following amended paragraph:

"FIG. 12A is a diagram showing another embodiment of the system of the invention having an S-box located in a designated portion of memory in the cipher subprocessor of FIG. 7C."

For the paragraph beginning on page 9, line 19, please substitute the following amended paragraph:

"**DETAILED DESCRIPTION OF ~~DRAWINGS~~ THE INVENTION**"

For the paragraph beginning at page 9, line 20, please substitute the following amended paragraph:

"FIGS. 7A, 7B, and 7C ~~is a~~ depict block diagrams showing an example hardware configuration of the system of the invention having an optimized cipher subprocessor 700, 1100, 1200. As shown in FIGS. 7A, 7B, and 7C, data 602 and a key 618 may be input to a control unit 601 by way of 32-bit interfaces. The data 602 may be stored in a 128-bit input register 604, which, in subsequent rounds of the AES algorithm, may be used to store intermediate states or intermediate cipher texts. For convenience, the initial plain text and the intermediate cipher text will be referred to herein as "intermediate states," "state data," or simply "states." The state, which is stored in the 128-bit input register 604, may be input to an optimized cipher subprocessor (or cipher core or cipher subsystem) 700, 1100, 1200 via 32-bit data buses 613 in a sequential manner. The

encryption (or decryption) process takes place simultaneously as the states are being loaded into the optimized cipher subprocessor 700, 1100, 1200. In other words, unlike the system of the prior art, it is no longer necessary to wait for complete loading of the state before manipulating the state. The optimized cipher subprocessor 700, 1100, 1200 may also be configured to improve performance with respect to the ByteSub step of the AES algorithm. This aspect of the optimized cipher subprocessor will be discussed in greater detail below. Once encryption or decryption is complete, the cipher text may be written to a 128-bit output register 608 via 32-bit data buses 614 in a sequential manner. In one non-limiting embodiment of the invention, the cipher may be managed using a control register containing an encryption/decryption flag (not shown), run flag (not shown), and a reset bit (not shown). In such a non-limiting environment, data and control registers may be accessible using /CS_DATA 622 and /CS_CTRL 624 signals, and read and write may be realized at the rising edge of /READ 632 and /WRITE 628 signals, respectively. Key memory may be organized in 256 32-bit words, and pre-calculated sub-keys may be entered to the cipher via a separated 32-bit local interface that can be connected, for example, to the local memory. Furthermore, as shown in FIG. 7A, 7B, and 7C, new sub-keys may be written to the internal memory at the rising edge of a KEY_STRB 638 signal when /WR_KEY 634 is low. As seen from FIG. 7A, 7B, and 7C, the cipher subprocessor 700, 1100, 1200 increases efficiency by allowing state data manipulation as the state data is moved from main memory to the cipher subprocessor 700, 1100, 1200 memory. This is shown in greater detail in FIGS. 8A through 8I."

For the paragraph beginning on page 24, line 8, please substitute the following amended paragraph:

"FIG. 11A is a diagram showing another embodiment of the system of the invention having a hardwired S-box 1150 within the cipher subprocessor 1100 of FIG. 7B. In the embodiment of FIG. 11A, the cipher subprocessor 1100 comprises a memory access unit 1120 having a host direct memory access (DMA) unit 801 and a staggered FIFO 811. Unlike the embodiment of FIG. 8A, the cipher subprocessor 1100 here does not have a cipher DMA in the memory access unit 1120. Since the detailed structure and operation of the staggered FIFO 811 have been discussed above with reference to FIGS. 9A through 9H, they will not be discussed here. It is, however, worthwhile to note again that the staggered FIFO 811 allows the cipher subprocessor 1100 to perform the ShiftRow step of the AES algorithm on a given data set as the data set is being loaded into memory. The cipher subprocessor 1100 further comprises a hardwired S-box 1150, a first multiplexer (MUX) 830, a first data memory bank (hereinafter also referred to as cipher data memory bank 0, or, simply, bank 0) 850, a second data memory bank (hereinafter also referred to as cipher data memory bank 1, or, simply, bank 1) 860, a second MUX 870, a set of processing circuitry 831, and a third MUX 840. Similar to the configuration of FIG. 8A, the processing circuitry 831 of the cipher subprocessor 1100 is configured to perform the ByteSub step, the ShiftRow step, the MixColumn step, and the AddRoundKey step of the AES algorithm."

For the paragraph beginning on page 26, line 18, please substitute the following amended paragraph:

"FIG. 12A is a diagram showing yet another embodiment of the system of the invention having an S-box 1250 located in a designated portion of memory 841 in the cipher subprocessor 1200 of FIG. 7C. In the embodiment of FIG. 12A, the cipher subprocessor 1200 comprises a memory access unit 1120 having a host direct memory access (DMA) unit 801 and a staggered

FIFO 811. Since the detailed structure and operation of the staggered FIFO 811 have been discussed above with reference to FIGS. 9A through 9H, they will not be discussed here. It is, however, worthwhile to note again that the staggered FIFO 811 allows the cipher subprocessor 1200 to perform the ShiftRow step of the AES algorithm on a given data set as the data set is being loaded into memory. In addition to the memory access unit 1120, the cipher subprocessor 1200 further comprises a memory location 841 having the S-box 1250, and a RAM access unit 1275 configured to retrieve the S-box 1250 from the cipher subprocessor memory. In all other respects, the cipher subprocessor of FIG. 12A comprises the same hardware components as FIG. 8A. Thus, the hardware components will be further discussed with reference to FIGS. 12B through 12I, which show their operation."